Dell Technologies Supply Chain Security: Secured Component Verification for PowerEdge

Tech Note by

Craig Phelps
Kim Kinahan
Mukund Khatri
Jason Young

Summary

A core element of Dell Technologies' security-enabled supply chain program is Secured Component Verification (SCV), now an integral part of the entire PowerEdge Server line.

SCV enables end-users to validate that systems delivered are secure, that components and configurations set at time of manufacture conform to the specifications set by the customer, and remain so throughout the journey, from factory to data center.

Introduction

Dell Technologies has long known that a secure product begins with a secure supply chain and has had a robust Supply Chain Assurance Program for many years. As the threat landscape becomes more complex and sophisticated, so too system protection and control measures need to evolve to meet the challenge. Systems can be vulnerable to hardware intrusion or manipulation in the form of undetectable malware inserted during manufacturing or during transit from the factory. From the moment a server leaves the factory until it arrives at its destination, it is potentially exposed to security threats without the user even realizing what is happening, such as counterfeit components, malware and firmware tampering.

Organizations understand the importance of a secure supply chain and are making purchasing decisions with that in mind. Addressing this industry-wide concern for customers, Dell Technologies is adding new supply chain security offerings for the entire Dell EMC PowerEdge Server portfolio, strengthening the integrity of the hardware and expanding its comprehensive secure supply chain practices.

Dell Technologies Secure Supply Chain

Dell Technologies takes a multifaceted approach to protect its supply chain and to deliver solutions that customers can trust. Whether it's a desktop, laptop, server, or a data storage array, product features are conceived, designed, prototyped, implemented, set into production, deployed, maintained and validated with supply chain security as a top priority.

As a safeguard, Dell has 'cybersecurity-hardened' the entire server development lifecycle, from design and development, through manufacturing, to delivery and use in ways that span the entire PowerEdge portfolio.

Some of the Key measures in place to enable broad supply chain assurance are:

- chain of custody tracking and anti-tamper packaging
- 3rd party access restrictions and staff checks at point of manufacturing
- code signing and secure downloading
- chain of trust maintenance for critical components
- hardware intrusion detection, and recording of enclosure breaches during shipmen

Through trusted relationships, and high standards of responsibility and integrity for ourselves and across our supply chain network, we drive reliable manufacturing that our stakeholders can trust.

In total, these measures serve as important differentiators for Dell EMC customers, especially in the Federal, Banking/Finance, Healthcare and Retail sectors.

Dell Technologies Secured Component Verification

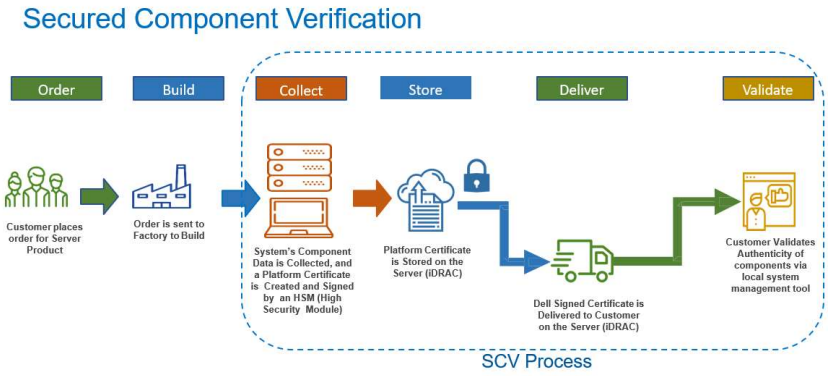
A core element of Dell's security-enabled supply chain program is Secured Component Verification (SCV), now an integral part of the entire PowerEdge portfolio, and soon to come to other product lines.

Dell Technologies Secured Component Verification for PowerEdge provides verification of the as-built hardware configuration for PowerEdge servers. The verification enables customers to confidently deploy new servers in their datacenters knowing the hardware integrity is in-tact from the outset and that the chosen configuration will provide them with a solid foundation for their mission critical applications.

SCV enables IT administrators to validate the componentry of incoming systems to ensure that the configuration is identical to what has been manufactured, and that components and configurations set at time of manufacture, conform to the specifications set by the customer, and remain so throughout the journey, from factory to data center. Any component changes that occur after a device leaves the Dell factory, and before the verification is run, will show up as a mismatch in the resulting report. This allows customers to account for authorized changes and to identify unauthorized changes.

A cryptographic certificate is generated in the factory, capturing component data at the point of origin, that contains specific component data and corresponding unique identifiers. It is securely stored in the server and is later validated against the as-received configuration by the customer at point of arrival. This is achieved via an application that assesses the as-received componentry and associated unique ID's. SCV conforms to Federal supply chain crypto requirements to meet future standards.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.
Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries



Validation through Application

When a customer purchases a server with an SCV license, it is built to order with validated components. At time of manufacture, each critical server part is analyzed, a unique ID is recorded, which includes a set of component data. The specific manufactured hardware configuration is captured within a cryptographic certificate that is bound to the unique server. This SCV certificate is signed by a Dell Certificate Authority and stored in iDRAC, to be retrieved by the customer or by the Dell SCV Validation application. The manufactured hardware configuration is cryptographically locked to the certificate and will accompany the server during transit to the customer.

When a customer brings a new server into their environment and powers it up, they can run the SCV Validation app to collect and compare the current hardware configuration against the hardware configuration collected at the time it was built in the Dell factory. The result is either a perfect match, or a list of components not in compliance with those used at time of build.

In Conclusion

The Dell Technologies Secured Component Verification (SCV) enables IT administrators to validate what Dell has manufactured and track any expected or unexpected hardware modifications that have occurred during the journey from the factory to datacenter.

Using SCV, IT operations and security teams gain assurance that just-delivered systems conform to component specifications, and that potential attack vectors have been much reduced. They can now spend more time focusing on supporting business outcomes and let Dell help them provide assurance and confidence with their server infrastructure.

PowerEdge DfD Repository
For more technical learning

Contact Us
For feedback and requests

Follow Us
For PowerEdge news